Claims

Sub B1

1. Method for personalizing GSM chips having a memory range in which at least one subscriber identification number IMSI and a card number ICCID are stored, and wherein for personalizing the chip an additional secret key Ki and, optionally, additional data are stored,
characterized in that the chip is personalized at the time when the subscriber logs on to the subscriber network.

2. The method according to claim 1, characterized in that the chip is personalized when the subscriber logs on to the subscriber network for the first time.

3. The method according to claim 1 or 2, characterized in that for pre-personalizing the chip at the manufacturer, at least initial, card-specific data, namely a first secret key Ki_1 and, optionally, additional data, such as PIN and PUK are stored.

4. The method according to one of the claims 1-3, characterized by the following process steps:

in a first process step, the chip manufacturer obtains the ICCID and the IMSI from a number pool, the chip itself derives an initial key Ki_1 from a key K1 which is known to and entered into the chip by the chip manufacturer, while PIN and PUK are set to a default value,

in a second process step, an entry is made in the AC and HLR as soon as a subscriber has entered into a contract with the network operator,

in a third process step, the AC also derives the initial first key Ki_1,

in a fourth process step, the network sets the conditions so that during logon to the network, a connection is established from the chip to the component SC (security center of the network operator),

in a fifth process step, the connection is routed from the chip to the SC during the first logon,

in a sixth process step, a new, second secret key Ki_2 and, optionally, a PUK is negotiated with the chip (for example using the Diffie-Hellman method) or generated in the SC and transmitted to the chip,

in a seventh process step, the conditions of the fourth process step are disabled again.

5. The method according to one of the claims 1-4, characterized in that the initial secret key Ki_1 which is first stored in the chip, is not transmitted to and stored in the authentication center (AC) before the contract is established.

6. Chip for carrying out the method according to one of the claims 1-5, characterized in that the chip in the terminal equipment is Toolkit-enabled and can communicate with the SC and negotiate a key.

7. The chip according to claim 6, characterized in that the chip can receive data from the SC and writes these data to its memory and, optionally, reads these data from the memory the and changes the data and/or transmits the data to the computer center (SC).

8. The chip according to one of the claims 6 or 7, characterized in that the micro-processor of the chip negotiates a secret key with the SC.

9. The chip according to claim 8, characterized in that the key of the method is negotiated using the Diffie-Hellman method.

10. The chip according to one of the claims 6-9, characterized in that the chip has a dialing number which is fixedly pre-programmed by the manufacturer (fixed dialing).

11. Computer center for carrying out the method according to one of the claims 1-5, characterized in that the HLR is capable of setting and deleting a rerouting command (hotlining flag).

12. Computer center for carrying out the method according to one of the claims 1-5, by using a chip according to one of the claims 6-10, characterized in that the network sets conditions so that a connection is established from the chip to the component SC during logon to the network.

13. Computer center for carrying out the method according to one of the claims 1-5, by using a chip according to one of the claims 6-10, characterized in that the hotlining flag is set in the HLR when the initial key Ki_1 is a first entered in the AC.